UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/385,589	08/29/1999	GARY L. GRAUNKE	42390.P7574	9393

7590 05/06/2003

ALOYSIUS T C AUYEUNG
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
7TH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
GURSHMAN, GRIGORY	
ART UNIT	**PAPER NUMBER**
2132	11

DATE MAILED: 05/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/385,589	GRAUNKE ET AL.	
	Examiner	Art Unit	
	Grigory Gurshman	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 August 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 August 1999* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2,3,4,6* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Drawings

1. The drawings are objected to because of draftsperson's objections (see PTO 948). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Objections

2. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not). Misnumbered claims 14-28 have been renumbered 16-30 respectively.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claim 16 is rejected under 35 U.S.C. 102(e) as being anticipated by Shukla (U.S. Patent No.6.345.101 B1).

4. Referring to claim 16, Shukla discloses a cryptographic method for data communication and storage (see abstract). Shukla teaches XOR operations along with shuffling data blocks (see column 2, lines 55-56). The limitation "a first XOR gate to

receive a first plurality of data bits and combine them into a second data bit" is met by XOR operation of the data block D with the string S to obtain a new data block D1(see column 3, lines 12-14). The limitation "shuffle units, coupled to the first XOR gate, to output a third data bit by shuffling the second data bit through the network of shuffle units" is met by the second operation, which shuffles the bits of the data block D1 to obtain a new data block D2 (see column 3, lines 14 -16). The limitation " a second XOR gate coupled to the network of shuffle units to combine a fifth plurality of data bits using the third data bit" is met by the a second type of XOR that uses the bits of the data block D2 and produces the data block D3 (see column 3, lines 16-18). Shukla explicitly shows the limitations, recited in the independent claim 26, in Fig. 3.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1 -15 and 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski (U.S. Patent No. 5.341.425) in view of Richard (U.S. Patent No. 4.004.089).

7. Referring to the instant claims, Wasilewski discloses a method for uniquely encrypting data (see abstract). Wasilewski shows a system (see 130 in Fig.5) comprising data bit generator. The generator generates 1-n plurality of data bits (see

unit 154), which meets the limitation "data bit generator to generate a first, second and third plurality of data bits", recited in claim 1. The limitation "a combiner function, coupled to at least one data bit generator" is met by combiner (see unit 156 in Fig.5). The limitation "to combine the third plurality of data bits, using the first and second plurality of data bits as first input data bits and control signals" is met by the data stream 158 (Fig. 5). Wasilewski, however, does not explicitly teach a combiner including a network of shuffle units. Richard discloses a cryptic device for enciphering and deciphering data (see abstract). Richard teaches generating pseudorandom bit sequence. Richard also teaches the means for combining the generated bit sequence with a clear text data bit signal and shuffling means, which receives the encoded signal and shuffles the positions of the bits within the signal (see column 2, lines 50 -57 and Fig. 4A unit 160). Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to modify the combiner coupled to a data bit generator of Wasilewski by adding the shuffle units as taught in Richard. One of ordinary skill in the art would have been motivated to modify the combiner coupled to a data bit generator by adding the shuffle units as taught in Richard for providing the fully encoded signal (see Richard, abstract and column 2, lines 56-60).

8. Referring to claim 26, Wasilewski teaches generating n-number of pluralities of data bits (see Fig 5), which meets the limitation "fourth data bit generated from the first plurality of data bits ... to output a fifth data bit to combine third plurality of data bits."

9. Referring to claims 9 -12, Wasilewski teaches that combiner comprises an exclusive-OR (XOR) gate (see column 1, lines 49-52).

10. Referring to claim 14, it is well known in the art to use a data bit generator comprising a plurality of LFSRs. One of ordinary skill in the art would have been motivated to create a data bit generator comprising a plurality of LFSRs for generating different pluralities of data bits.

11. Referring to claims 2-8, Richard teaches shuffle unit, which comprises flip-flops (see unit 164 in Fig 4A and units 73 and 74 in Fig 2A). The plurality of selectors coupled to the flip-flops is met by units 70, 71, 75 and 72 in Fig 2A).

12. Claims 17-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shukla (U.S. Patent No.6.345.101 B1) in view of Richard (U.S. Patent No. 4.004.089).

13. Referring to the instant claims, Shukla discloses a cryptographic method for data communication and storage (see abstract). Shukla teaches XOR operations along with shuffling data blocks (see column 2, lines 55-56). Shukla teaches the use of shuffle units (see Fig. 3). Shukla, however, does not explicitly teach shuffle unit comprising flip-flops for string state values. Richard discloses a cryptic device for enciphering and deciphering data (see abstract). Richard teaches the means for combining the generated bit sequence with a clear text data bit signal and shuffling means, which receives the encoded signal and shuffles the positions of the bits within the signal (see column 2, lines 50 -57 and Fig. 4A unit 160). Richard also teaches a shuffle unit, which comprises flip-flops (see unit 164 in Fig 4A and units 73 and 74 in Fig 2A) coupled to selectors (units 70, 71, 75 and 72 in Fig 2A). Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to modify the shuffle

units coupled to XOR gates of Shukla by adding the flip-flops coupled to the selectors as taught in Richard. One of ordinary skill in the art would have been motivated to modify the shuffle units coupled to XOR gates by adding the flip-flops coupled to the selectors as taught in Richard for controlling the mode of operation of Shuffle Register.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (703) 306-2900. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the TC 2100 receptionist whose telephone number is (703) 305-3900.

Grigory Gurshman
Examiner
Art Unit 2132

GG
April 29, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100